Security, Compliance, Privacy, and Trust

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

DESCRIBE GENERAL SECURITY AND NETWORK SECURITY FEATURES

✓ **Describe Azure security features**

- Describe basic features of Azure Security Center, including policy compliance, security alerts, secure score, and resource hygiene
- Describe the functionality and usage of Key Vault
- Describe the functionality and usage of Azure Sentinel
- Describe the functionality and usage of Azure Dedicated Hosts

DESCRIBE GENERAL SECURITY AND NETWORK SECURITY FEATURES

✓ **Describe Azure network security**

- Describe the concept of defense in depth
- Describe the functionality and usage of Network Security Groups (NSG)
- Describe the functionality and usage of Azure Firewall
- Describe the functionality and usage of Azure DDoS Protection

DESCRIBE IDENTITY, GOVERNANCE, PRIVACY, AND COMPLIANCE FEATURES

✓ **Describe core Azure identity services**

- Explain the difference between authentication and authorization
- Define Azure Active Directory
- Describe the functionality and usage of Azure Active Directory
- Describe the functionality and usage of Conditional Access, Multi-Factor Authentication (MFA), and Single Sign-On (SSO)

DESCRIBE IDENTITY, GOVERNANCE, PRIVACY, AND COMPLIANCE FEATURES

✓ **Describe Azure governance features**

- Describe the functionality and usage of Role-Based Access Control (RBAC)
- Describe the functionality and usage of resource locks
- Describe the functionality and usage of tags
- Describe the functionality and usage of Azure Policy
- Describe the functionality and usage of Azure Blueprints
- Describe the Cloud Adoption Framework for Azure

DESCRIBE IDENTITY, GOVERNANCE, PRIVACY, AND COMPLIANCE FEATURES

✓ **Describe privacy and compliance resources**

- Describe the Microsoft core tenets of Security, Privacy, and Compliance
- Describe the purpose of the Microsoft Privacy Statement, Product Terms site, and Data Protection Addendum (DPA)
- Describe the purpose of the Trust Center
- Describe the purpose of the Azure compliance documentation
- Describe the purpose of Azure Sovereign Regions (Azure Government cloud services and Azure China cloud services)

DESCRIBE CORE SOLUTIONS AND MANAGEMENT TOOLS ON AZURE

✓ **Describe Azure management tools**

- Describe the functionality and usage of Azure Advisor
- Describe the functionality and usage of Azure Monitor
- Describe the functionality and usage of Azure Service Health

Chapter 3, “Azure Core Networking Services,” introduced several key networking concepts and Azure networking resources. This chapter expands on those concepts to describe Azure services and resources that enable you to apply various security methods to protect network traffic between Azure and your services and users. Topics covered in this chapter include Azure Firewall, network security groups, application security groups, user-defined routes, and Azure DDoS Protection.

This chapter also describes the key security-related topics of authentication and authorization, differentiating the two, and covers Azure AD and multifactor authentication. Continuing the security focus, the chapter explores Azure services, including Azure Security Center, Azure Key Vault, and Azure Information Protection.

This chapter also introduces several governance topics covered in the exam, including initiatives and policies, controlling access with role-based access control (RBAC), locking resources, and using Azure Advisor and Azure Blueprints. Reporting and monitoring options are also included.

The chapter rounds out with a discussion of compliance and data protection standards to help you begin to understand how to implement compliant solutions in Azure, as well as topics relevant to governmental and geopolitical requirements.

Network Security

Chapter 3 laid the foundations for understanding networking concepts and described resources and services in Azure that provide for networking Azure resources, securing network traffic with VPN options, connecting your data centers to Azure, using load balancing, and moving content close to your users with content delivery networks (CDNs). This chapter turns the focus from networking to resources and service in Azure that help secure your networks and network traffic.

Before exploring specific Azure services for networking security, let’s discuss an underlying concept: *defense in depth*.

Defense in Depth

Bad actors have many ways to compromise an organization’s security, from physical access to your building and facilities to attacks on your IT services and user devices. These attacks can come in many forms. Protecting against these bad actors is therefore obviously more difficult than simply deploying a firewall or ensuring your users have an antivirus application installed on their devices. This is where the concept of defense in depth comes into play.

Defense in depth defines a strategy for multiple layers of defense to protect your facilities, data, services, and users from compromise. These defense layers begin with physical security and extend to multiple points of potential compromise. The following list summarizes the key defense layers:

- **Physical security:** Controlling physical access to your facilities, including offices, data centers, and ancillary facilities such as warehouses and manufacturing plants, is critical to prevent unauthorized access to data in multiple forms and to servers, user devices, and other potential points of physical compromise.
- **Identity and access:** This layer protects services and data by ensuring that only authenticated users can access resources and that authorization ensures users can access only those resources allowed to them. Protection options include but are not limited to access control, single sign-on, multifactor authentication, and auditing.
- **Perimeter:** The perimeter of your network is the first point at which bad actors can potentially gain access to servers and other resources or execute attacks against your network. Firewalls help prevent intrusion, and services such as Azure DDoS Protectioncan guard against large-scale attacks.
- **Network:** Even within an internal network that is protected at the perimeter by a firewall, it's important to protect against potential threats. This includes ensuring that traffic can flow only between allowed endpoints, denying access by default and allowing access by exception only, highly restricting incoming access, limiting outbound traffic as necessary, and ensuring a highly secure connection between your on-premises networks and Azure.
- **Compute:** At this layer it is important to limit and secure access to servers, implement endpoint protection on all virtual servers, and ensure that all systems are patched against all potential threats.
- **Application:** At this layer protection begins with developing applications with security as the first and primary consideration. Third-party applications should be kept patched against vulnerabilities. You can use Azure Key Vault to protect secrets used by your applications.
- **Data**: This layer applies protection to your data in multiple locations, including databases and storage.

The specifics of fully implementing protection at each of these layers goes beyond the scope of this book and of the AZ-900 exam. However, the Azure services that are key to developing and implementing a defense-in-depth strategy are covered through the remainder of this chapter.

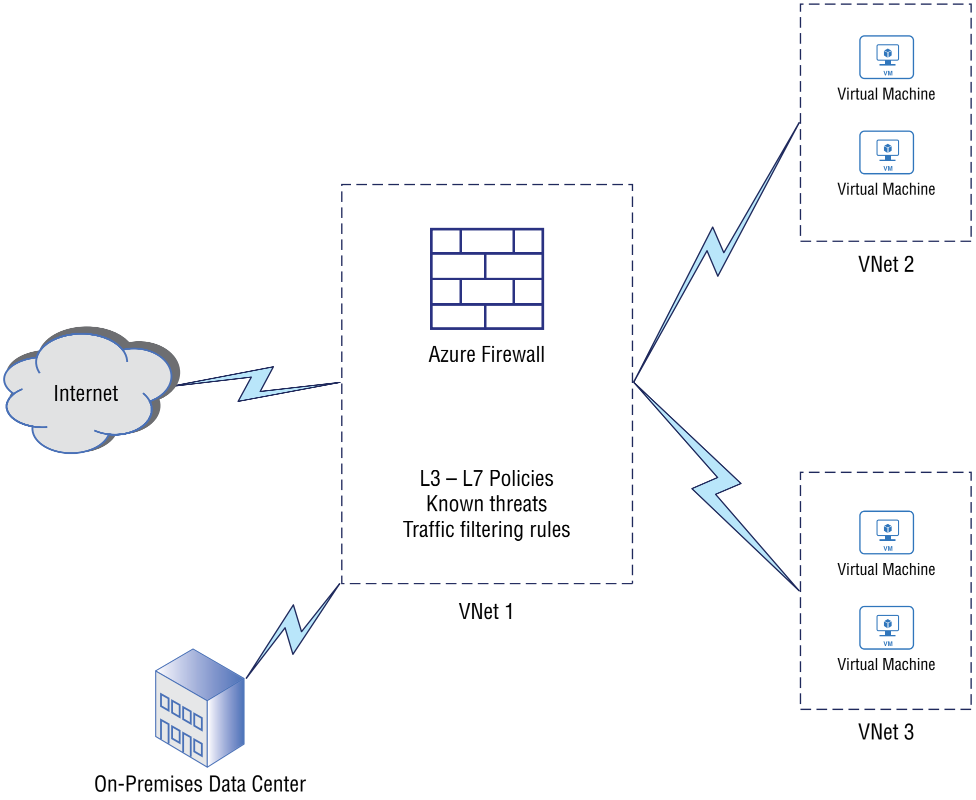
Azure Firewall

A *firewall* is a device or service that inspects network traffic flowing through it and applies actions to that traffic based on rules that you specify. Firewalls protect networks from intrusion and different types of network attacks. For example, if the only endpoints that you need to serve to your users are HTTP (port 80) and HTTPS (port 443), you would create a rule in your firewall to block all traffic inbound for ports other than 80 and 443. Firewalls can provide other capabilities as well. For example, some firewalls analyze network traffic for viruses, worms, and other network-borne threats.

Azure Firewall is a managed firewall service. It is a *stateful* firewall in that it inspects sessions of network traffic and can act based on the context and state of the packets. By contrast, a stateless firewall inspects individual data packets and is more limited in the information it gleans and therefore the actions it can take.

Azure Firewall can filter traffic based on several criteria, including port number, protocol type, network address, and fully qualified domain name (FQDN), among others. You create rules to specify how Azure Firewall will treat incoming and outgoing network traffic. If the traffic matches a rule that denies that type of traffic, the traffic is blocked. If the traffic matches a rule that allows that type of traffic, the traffic is allowed to flow through the firewall. If no rule applies, the traffic is blocked (denied). The firewall can also modify the traffic—for example, changing the source or destination addresses to route traffic. This latter mechanism is known as network address translation (NAT) and enables traffic to be routed between different network segments. Figure 4.1 illustrates an example of Azure Firewall in use.

FIGURE 4.1 Use Azure Firewall to scan and filter network traffic.



TIP

A fully qualified domain name uniquely identifies a host on a network, incorporating the hostname itself and the full domain name in which it resides. An example of a FQDN is `www.microsoft.com`, where `www` is the host and `microsoft.com` is the domain. If a host resides in a subdomain, the FQDN would include the subdomain, such as `owa.mail.microsoft.com`.

Azure Firewall supports three types of rule collections:

- **NAT rules:** As explained previously, NAT rules enable traffic to be forwarded between network segments, such as from the Internet to Azure resources.
- **Network rules:** These rules allow or deny traffic based on protocol type, inbound or outbound address, and inbound or outbound port.
- **Application rules:** These rules allow specific applications to communicate across the firewall and control traffic by FQDN. For example, you could block traffic to a specific website using an application rule.

TIP

Azure Firewall supports FQDN tags to simplify traffic routing. An FQDN tag represents a group of FQDNs that are associated with well-known Microsoft services. For example, you might use an FQDN tag in a rule to allow Windows Update traffic through Azure Firewall. Microsoft manages the FQDN tags, and you only need to include a tag in a firewall rule to allow the appropriate traffic.

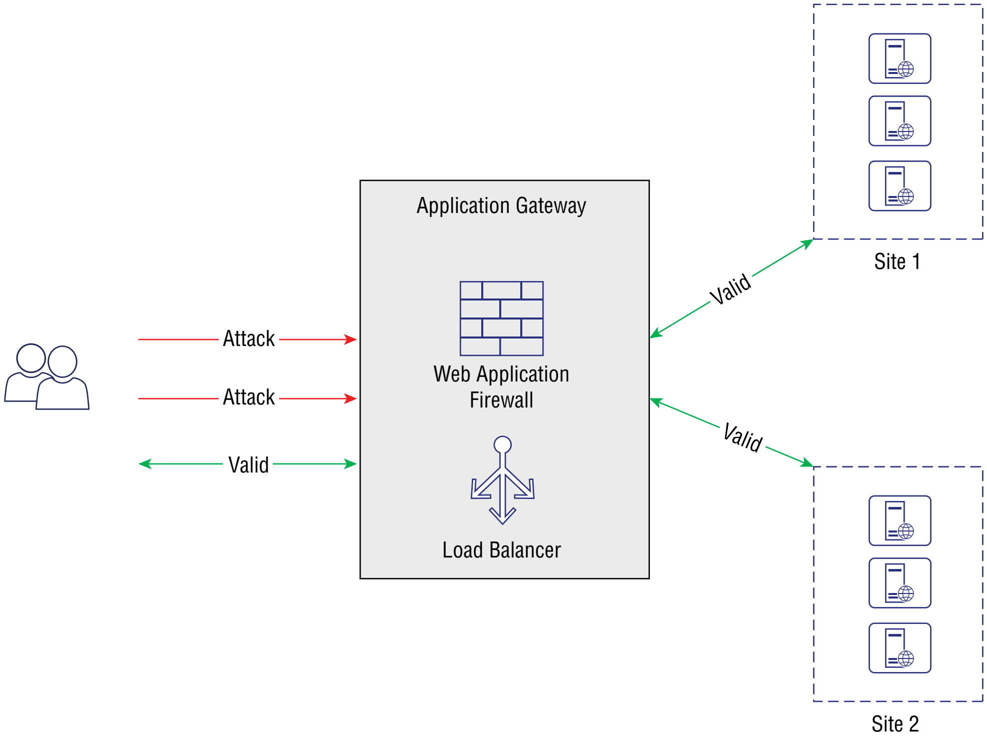
In the context of the AZ-900 exam, consider Azure Firewall whenever you need to filter traffic based on source IP address and port, destination address and port, and/or protocol. Azure Firewall is not specific to certain types of applications. For example, it is not limited to filtering traffic only for web applications.

Web Application Firewall

Chapter 3 described the load-balancing offerings of Azure Application Gateway and Azure Front Door, as well as Azure Content Delivery Network (CDN). Azure Web Application Firewall (WAF) is a firewall service that you can deploy with each of these services to provide firewall services specifically for your web applications. WAF provides features tailored to each of these services. Figure 4.2 illustrates WAF being used with Application Gateway.

WAF protects your web applications against common vulnerabilities and exploits, such as SQL injection and cross-site scripting. As with Azure Firewall, policies and rules determine how WAF functions in each deployment. WAF offers Azure-managed rules, which are preconfigured rules that you can deploy easily to guard against common threats. You can also create custom rules as needed.

FIGURE 4.2 Web Application Firewall works in conjunction with the Application Gateway, Front Door, and CDN services.

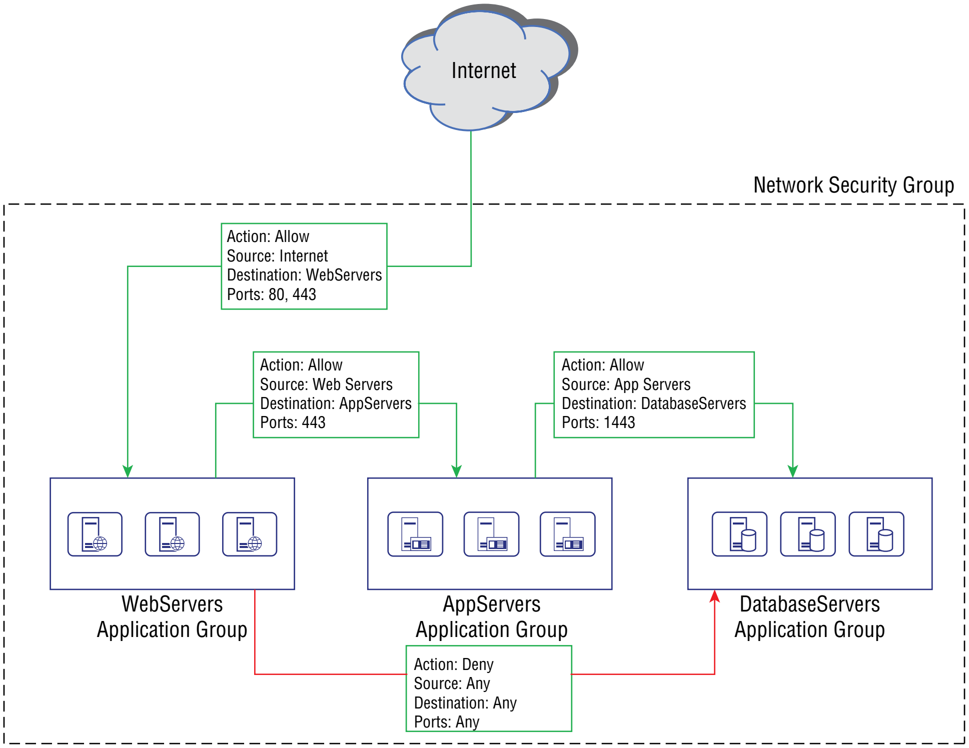


The key points to understand about WAF in the context of the AZ-900 exam are that it works in concert with Application Gateway, Front Door, and CDN, and it is specific to web application scenarios. If you are looking to protect other services and resources, turn to Azure Firewall and/or the additional network security services described in the following sections.

Network Security Groups

Network security groups (NSGs) are an additional firewall service offered in Azure. NSGs enable you to filter network traffic between Azure resources in an Azure virtual network. An NSG can be scoped to a subnet or to a network interface on a VM, and a single NSG can apply to multiple VMs or subnets. As with other Azure firewall services, you can create rules to determine which actions an NSG will take. NSGs also have default rules applied to them to allow communication between resources in a virtual network. NSGs can filter traffic based on protocol, source IP address, source port, destination IP address, and destination port. Figure 4.3 illustrates an implementation of an NSG. The NSG applies to all VMs within the subnet.

FIGURE 4.3 A network security group is a simple firewall offering in Azure.



Your Azure implementation will likely incorporate various levels of protection using many, if not all, of the firewall- and security-related services available in Azure to provide defense in depth. For example, if you do not host any web applications in Azure, the Azure Firewall might be the only solution you choose. But you might use Azure Firewall as a frontline defense with NSGs and application security groups (discussed in the next section), providing further protection for specific applications and networks. Or you might use Application Gateway in concert with NSGs to protect networks where web applications are hosted without employing Azure Firewall. The key point is that you must consider protection at multiple levels within your Azure environment and implement the service or combination of services that offers the appropriate protection.

In the context of the AZ-900 exam, keep in mind that NSGs provide protection at the subnet or individual VM level and are often deployed using application security groups, which are discussed next.

Application Security Groups

An application security group (ASG) enables you to group servers based on the applications running on them and then manage security for them as a group. The ASG is an object reference within a network security group, enabling you to easily apply the rules in the NSG to the virtual machines contained in the ASG. So, rather than apply a network security group to specific VMs where application servers reside, you create the ASG and add VMs to it, and then create the NSG and reference the ASG in it. The NSG rules then apply to the VMs in the ASG.

ASGs simplify how you apply NSGs to virtual machines. For example, you create an ASG and reference one VM in it. Then you create an NSG and reference the ASG in it. Now, that one VM in the ASG has those rules applied to it. All you need to do to apply the same NSG to a dozen other servers is to add them to the same ASG. Those servers now have the NSG applied to them.

User-Defined Routes

Chapter 3 described routing in general and how network traffic is routed between network subnets. When you define a subnet in Azure, Azure creates default routes to determine how resources in the subnet will communicate with resources in other subnets. Those routes are stored in a routing table that is used to determine the next hop for the traffic. Default routes work fine for many scenarios, but not for all. That is where user-defined routes (UDRs) come into play.

TIP

What is a network *hop*? Remember the discussion from Chapter 3 about your home network? When traffic from your wireless device hits the wireless access point (WAP), a routing table stored and managed by the WAP tells it where to send the traffic. Assume the traffic is destined for the Internet. The WAP determines that the destination address is a service on the public Internet and, based on its routing table, sends the traffic to the home router, which it knows is the next hop (the next waypoint on the traffic's journey) to the Internet. From there, the home router uses its own routing table to determine where to send the traffic. In this case, it sends the traffic to the ISP's router (the next hop). The process repeats until the network traffic reaches its destination.

A UDR enables you to define a custom route to override the default route. For example, assume you have a secure service hosted on a VM within a specific subnet and you want all traffic destined for that VM to go through a specific firewall instead of taking the default route. The target firewall is configured with rules to manage that traffic and scan it for certain vulnerabilities that would affect that specific VM. The solution is to create a UDR that directs traffic destined for the IP address of the VM through the firewall.

For the purposes of the AZ-900 exam, simply keep in mind that UDRs enable you to create a custom routing table and direct traffic through nondefault routes.

Azure DDoS Protection

As explored in Chapter 3, distributed denial-of-service (DDoS) attacks overwhelm a service by flooding the service with requests. When the number of requests increases significantly, the service's performance begins to suffer as resources are consumed. If enough requests are received by the service, it can fail altogether, making the service unavailable and denying access to the service (hence the name).

Azure DDoS Protection provides a means of defense against DDoS attacks. Azure DDoS guards against the following types of attacks:

- **Volumetric attacks:** These attacks flood an endpoint with a very large volume of traffic to overwhelm the service and/or consume all of the network bandwidth available within the network or between the endpoint and the rest of the Internet.
- **Protocol attacks:** These attacks target specific server resources through weaknesses in the protocol stack. An example is the Ping of Death attack, which floods the endpoint with ping requests, consuming service resources or overwhelming intermediate services such as the upstream firewall.
- **Resource layer attacks:** These attacks target the application layer of the protocol stack to affect web application traffic between hosts.

Azure provides DDoS Protection Basic and DDoS Protection Standard. The Basic offering provides active traffic monitoring and automatic attack mitigation. The Standard offering adds several other features, including an availability guarantee, mitigation policies, metrics and alerts, reporting, and more. So, if you only need detection and mitigation, Basic provides that function. When alerting, reporting, and customization are needed, DDoS Protection Standard is the appropriate offering.

Authentication and Authorization

The AZ-900 exam measures your knowledge about Azure Active Directory, authentication, and authorization. This section explores these topics, beginning with Azure Active Directory.

Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. Azure AD enables users to log into cloud services such as Microsoft 365 and access resources in Azure, including custom applications that you create and host in Azure. You can also use Azure AD to provide access for your users to resources hosted on-premises.

If you subscribe to Microsoft 365, Office 365, Azure, or Dynamics 365, you already have Azure AD because these subscriptions automatically get an Azure AD tenant with access to all of the free Azure AD services offered by Microsoft. You can also take advantage of paid Azure AD plans when you need additional capabilities. The following list explores these options:

- **Azure Active Directory Free:** This option provides management of users and groups, synchronization with on-premises Active Directory, basic reporting, self-service password change for accounts in Azure AD, and single sign-on (SSO) for Azure, Microsoft 365, Dynamics 365, and other applications hosted in the cloud.
- **Azure Active Directory Premium P1:** This option includes all features in Free along with the capability to access on-premises resources as well as cloud resources, support for dynamic groups, self-service group management, Microsoft Identity Manager, and cloud write-back to allow self-service password changes for on-premises users.
- **Azure Active Directory Premium P2:** P2 includes Free and P1 features along with Azure Active Directory Identity Protection for conditional access to apps and critical data, and Privileged Identity Management to discover, monitor, and restrict administrative access to resources.
- **Pay-as-you-go feature licenses:** Add other features to a pay-as-you-go tenant.

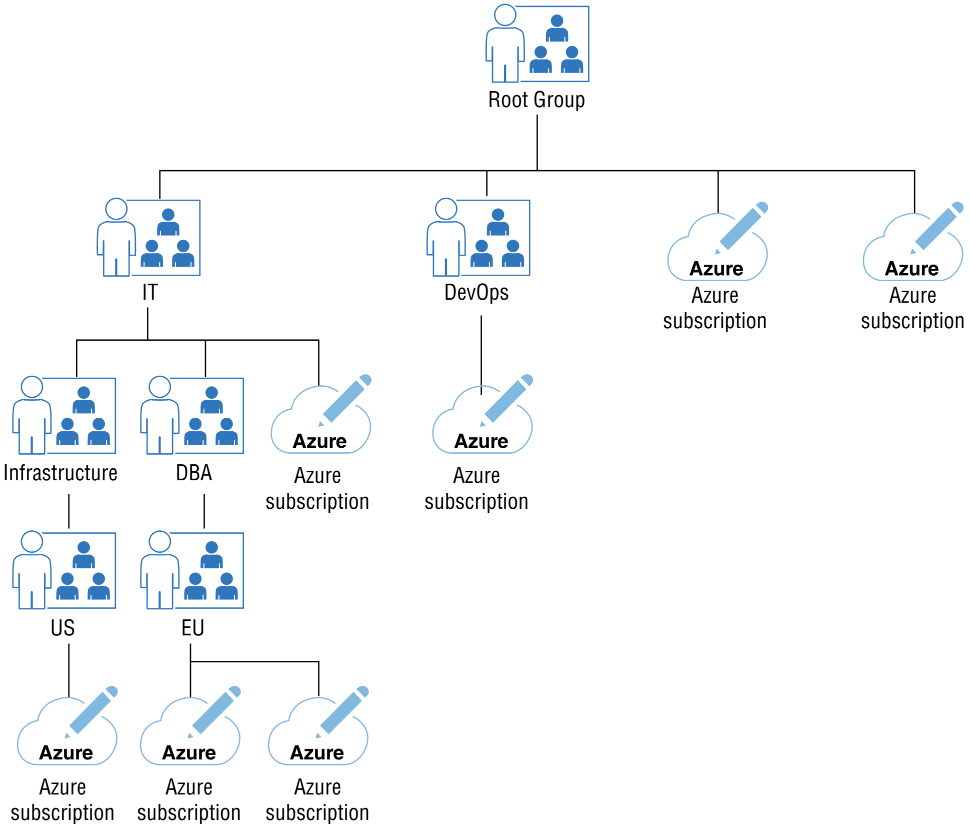
Regardless of which Azure AD offering you choose, you do not need to integrate with an on-premises Active Directory to use Azure AD for authentication and authorization. If all your IT resources are in the cloud and you host nothing on-premises, Azure AD can be your sole directory service. However, you can integrate with on-premises AD for hybrid cloud scenarios involving on-premises and cloud services by deploying Active Directory Federation Services (ADFS).

Azure AD supports role-based access control (RBAC) to manage access to cloud resources. With RBAC, you control who has access to specific Azure resources, what actions they can take with those resources, and what areas they can access.

To use RBAC in Azure, you create a role assignment that consists of a security principal, role definition, and scope:

- **Security principal:** Represents a user, group, service principal, or managed identity. A service principal is a representation of an application and is used to define the application's permissions. Managed identities provide services with the ability to authenticate to other Azure services without the need for a developer to create or manage identities or their credentials.
- **Role:** A collection of permissions that determine the actions that the role can perform, such as read, write, and delete. Azure offers built-in roles, and you can create custom roles where needed.
- **Scope:** The set of resources to which the access applies. You can specify scope in Azure at the management group, subscription, resource group, or resource level. A management group is a container for subscriptions, enabling you to organize and control management across multiple subscriptions. Figure 4.4 illustrates management groups.

FIGURE 4.4 Management groups serve as containers for subscriptions and enable you to control management across those subscriptions.



To sum up RBAC, the security principal describes who or what has a set of permissions, the role specifies the permissions that security principal has, and the scope defines where the security principal can use those permissions. So, Security Principal = who, Role = what, and Scope = where.

Authentication and Authorization

There is a difference between *authentication* and *authorization*, and the AZ-900 exam measures your knowledge of that difference. Simply put, authentication identifies a user and authorization determines the actions that an authenticated user can perform. It is a case of "who are you?" and "what can you do?"

In the context of Azure AD or on-premises Active Directory, a user's account identifies the user, providing authentication. So, when you provide a username and password, Azure AD authenticates you against those credentials. When you log into a website, you might submit your email address and a password to go with it. This is another example of authentication. Your debit card uses a form of authentication as well. The card number and numeric PIN that you enter to use the card in an ATM identify (authenticate) you. Presenting your passport to board a flight is another example of authentication because the passport identifies you.

As described earlier, authorization determines the actions you can take *after* you have been authenticated. Using your passport again as an example, the passport authenticates who you are, but it does not by itself allow you to travel to another country. A *travel visa* serves as your authorization to enter the country. Showing your birth certificate to prove that you are eligible for age-based benefits is another example of authorization because it lists your age (authorizing you for benefits) as well as identifying you.

Azure Multifactor Authentication

Multifactor authentication (MFA) is a mechanism that uses more than one *factor* to authenticate you. Assume your organization does not use MFA. To log on to the company intranet, you enter your username and password, and the site grants you access. This is single-factor authentication. The username itself does not authenticate you—providing the appropriate password does.

MFA increases security by requiring a second form of verification. For example, text messages are a common means of MFA. If your organization were using MFA in the previous example, you log on to the website and provide your username and password. The system then sends a text message to the mobile number it has on file for you with an access code. You enter the code into the browser, authenticating your identity. Passwords, voice calls, text messages, and verification emails are examples of methods that can be used to authenticate a user. When you use two or more methods, you are performing multifactor authentication.

Conditional Access

Conditional access is another tool you can use to secure access to Azure resources. Conditional access enables you to use various *identity signals* to allow or deny access to Azure resources in addition to authentication and RBAC (which is covered later in this chapter in the section "Role-Based Access Control"). Examples of identity signals include the user's location, the user's device, or the application the user is trying to access. Azure then uses these signals to determine what action to take. For example, if a user is logging in from a known office location (known network), you can configure conditional access rules to allow access without MFA. If the user tries to access a resource from an external network, MFA is used. Or, you might create a rule to require users to access specific resources only from a managed device.

You implement conditional access by creating conditional access policies that specify the appropriate identity signals and corresponding actions. Azure includes a What If tool that enables you to model conditional access policies and test them against recent login and access attempts from your users to determine what effect the policies would have had in those situations. The tool is therefore useful for testing your conditional access policies before you deploy them into production.

Conditional access requires an Azure AD Premium P1 or P2 license, or a Microsoft 365 Business Premium license.

Single Sign-On (SSO)

In a typical organization, almost all resources require authentication and authorization. For example, when you log on to an internal company portal, that portal very likely requires you to authenticate and prove not only that you are an employee but that you should have access to the portal. Now, imagine that in the course of your day you use a dozen or more resources, all of which require authentication and authorization. Providing your credentials every time you access a resource would be onerous, to say the least.

Single sign-on (SSO) enables you to use a single set of credentials to access multiple resources. For example, assume your organization has implemented SSO. You connect to a line-of-business application and instead of entering your credentials, the application uses your current user context to authenticate you and grant access automatically. Next, you open the company portal in a web browser. SSO performs the same task, authenticating you without you entering any credentials.

In many organizations, Active Directory on-premises stores user credentials. In order for a user at the office to authenticate in Azure without using a separate set of credentials, there needs to be a synchronization and coordination between AD on-premises and Azure AD. The primary tool that makes that possible is Azure AD Connect, which synchronizes changes between AD and Azure AD, providing a seamless authentication and access experience for the user. Azure AD Connect makes it possible to use not only SSO across both environments, but also MFA and self-service password reset.

Security Tools and Features

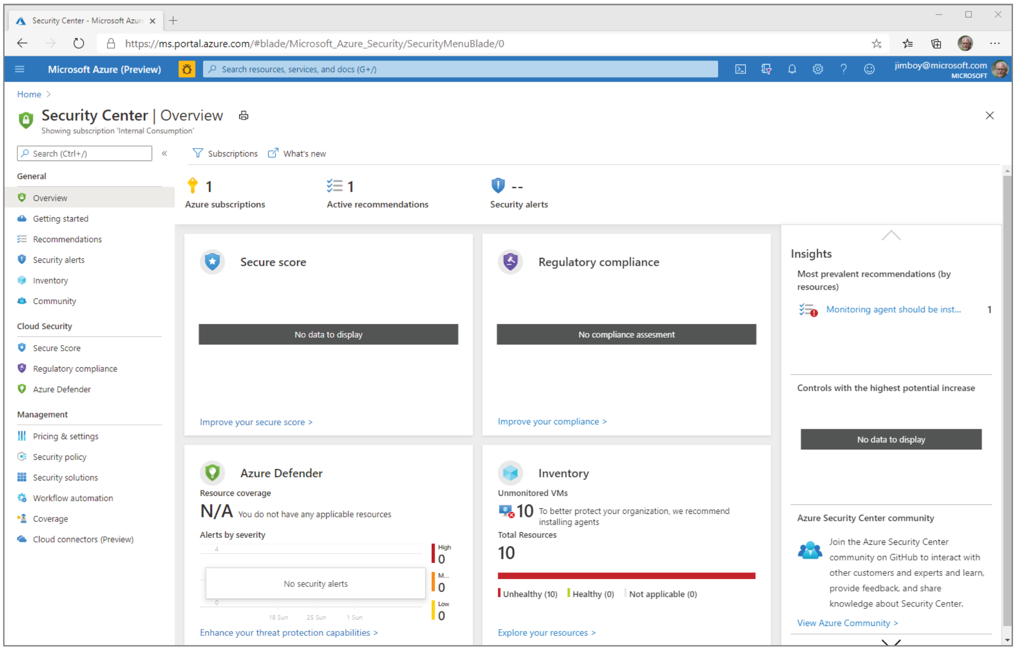
Azure includes several services to enable you to employ strong security within your Azure environment. This section explores the security services and features that are covered by the AZ-900 exam.

Azure Security Center

Azure Security Center (Figure 4.5) is a monitoring service that provides a framework for advanced threat protection of your IT workloads both in the cloud and on-premises. Azure Security Center strengthens your security posture by automatically assessing your environment for security risks and providing security-based monitoring, alerts, and recommendations. It can use machine learning to detect and block malware, and you can also create a whitelist of applications that can execute, blocking all others.

Security Center supports Azure-only environments, Azure and on-premises, Azure and other cloud offerings, as well as all three together: Azure, on-premises, and other clouds. Security Center supports both Windows- and Linux-based operating systems.

FIGURE 4.5 You access Security Center from the Azure portal.



Security Center - Microsoft Azure

https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/0

Microsoft Azure (Preview)

Search resources, services, and docs (G+/)

jimboy@microsoft.com
MICROSOFT

Home >

Security Center | Overview

Showing subscription 'Internal Consumption'

Search (Ctrl+/)

General
- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Community

Cloud Security
- Secure Score
- Regulatory compliance
- Azure Defender

Management
- Pricing & settings
- Security policy
- Security solutions
- Workflow automation
- Coverage
- Cloud connectors (Preview)

Subscriptions What's new

1 Azure subscriptions

1 Active recommendations

-- Security alerts

Secure score

No data to display

Improve your secure score >

Regulatory compliance

No compliance assesment

Improve your compliance >

Azure Defender

Resource coverage

N/A You do not have any applicable resources

Alerts by severity

No security alerts

High 0
M... 0
Low 0

Enhance your threat protection capabilities >

Inventory

Unmonitored VMs

10 To better protect your organization, we recommend installing agents

Total Resources

10

Unhealthy (10) Healthy (0) Not applicable (0)

Explore your resources >

Insights

Most prevalent recommendations (by resources)

Monitoring agent should be inst... 1

Controls with the highest potential increase

No data to display

Azure Security Center community

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center.

View Azure Community >

Security Center integrates natively with Microsoft Defender (formerly known as Windows Defender) to provide risk detection and assessment and threat intelligence. Security Center enables automated onboarding for new VMs that you deploy and automatically discovers and assesses resources when you deploy them.

Security Center is offered at two service levels:

- **Free:** This service tier is limited to assessments and recommendations only for Azure resources.
- **Standard:** This service tier provides a broad range of features for continuous monitoring and threat detection.

One feature of Security Center Standard is the capability to perform just-in-time (JIT) access control for ports. For example, assume that you need to occasionally query a database to build a custom report but the necessary ports are blocked. JIT would enable you to request access to those ports for a specified period. Once that period ends, the ports are closed again. JIT dramatically reduces the attack surface by closing ports until they are needed and keeping them open only as long as needed.

Security Center is designed to help you understand your security posture and improve it. A feature that is central to Security Center is *secure score*, which is displayed in a tile in the Security Center portal. The score provides an indication of the overall security posture across your environment, presented as a percentage. The higher your score, the lower the identified risk posture. In addition to viewing your secure score from the Security Center portal, you can access it through the REST API to display in other applications or sites or use Azure Resource Graph to access the score.

Using the secure score reports that Security Center surfaces through the portal, you can view what items have negatively affected your secure score and use that information to develop a remediation plan to improve your overall security posture in Azure.

Azure Key Vault

Many services and applications use certificates and other *secrets* for authentication, data connections, encryption, and so on. For example, imagine your organization has created a custom service that needs to communicate securely across your environment with other services. It would likely do so using credentials. Hard-coding credentials in an application puts those credentials at risk for compromise and makes key management difficult at best.

Azure Key Vault enables you to securely store secrets such as tokens, passwords, certificates, cryptographic keys, and API keys. Using the previous example, instead of storing the credentials in your custom application, you would store the credentials in Azure Key Vault. The application would call Key Vault whenever it needed to use the credentials. The detailed process and mechanisms are outside the scope of the AZ-900 exam, but the following brief overview will help you understand the process in a general way:

1. You register the application as a security principal in Azure AD.
2. You configure a role assignment in Azure AD for that security principal.
3. You configure access policies for that security principal in Key Vault.
4. If needed, you configure firewall access to enable the application to reach the Key Vault.
5. When the application is running and needs to access the credentials, it first authenticates with Azure AD to get an access token and then makes a call to Key Vault.
6. Key Vault calls Azure AD to validate the application's security principal's access token. If the token validates, Key Vault gives the secret to the application. Because the application is only using the secret at runtime, there is no need for the application to store it.

Azure Key Vault also provides a centralized, cloud-based service for creating, storing, and managing keys and certificates. By storing secrets in Key Vault, you gain the capability to easily monitor and audit access. You also gain the capability to easily use those secrets among many Azure services.

Azure Information Protection

Azure Information Protection (AIP) enables you to classify and protect documents and emails by applying labels to them. AIP labels can be created and managed by administrators for use by users, created by users, or created by users based on recommendations created and managed by administrators. The labels identify the information type and can be used to optionally protect the information with Azure Rights Management Service (Azure RMS). Azure RMS can apply policies for encryption, identity, and authorization to the data to control its use and distribution. For example, you might create a policy to prevent email from being forwarded. Applying the appropriate tag to the email would result in recipients of the email being unable to forward it.

The key point to understand about AIP is that it provides a means to classify documents and emails using labels and to optionally protect them with encryption, identity, and authorization.

Azure Advanced Threat Protection

Azure Advanced Threat Protection (ATP) leverages your on-premises Active Directory to detect and identify threats directed at your organization. It enables you to investigate those threats and identify compromised identities and malicious activities. With ATP you can protect identities and credentials stored in Active Directory, monitor users and suspicious activities, report on incidents to help drive protection and remediation measures, and more.

Some of the key threats that ATP will help you detect and deal with are as follows:

- **Reconnaissance attacks:** Attackers scan the network to locate assets and services they can compromise, such as usernames, group membership, and IP addresses. An example of such an attack is probing accounts using an alphabetical list of usernames.
- **Compromised credentials:** Attackers attempt to gain access with compromised credentials, such as a brute-force attack testing multiple passwords against a username.
- **Lateral account movement:** Attackers steal user data on one computer in order to gain access to other computers. Examples include stealing Kerberos tickets (pass-the-token), stealing a key (overpass-the-hash, also a Kerberos attack), and stealing NTLM data (pass-the-hash).
- **Domain dominance:** Attackers compromise the domain through activities such as remote code execution on the domain controller, malicious domain controller replication, and other domain-related attacks.

TIP

You can use ATP to notify you of attempts to use decoy accounts, commonly called *honeytoken accounts*. You set up an account that is never used and has no permissions (the decoy), and then configure ATP to alert you when that account shows activity.

Azure Sentinel

Gathering information and managing security events across your environment is critical for protecting your users and data. Systems that provide this broad capability are security information and event management (SIEM) systems. Azure Sentinel is Microsoft's Azure-based SIEM solution.

Azure Sentinel collects data across your enterprise from users, devices, applications, and infrastructure on-premises and in the cloud, including from multiple clouds. It uses a combination of built-in analytics, leveraging information about known threats, machine learning, and other criteria to automatically detect threats. You can also create custom rules to search for specific threat criteria.

Azure Sentinel uses analytics to correlate alerts from across the environment into incidents, enabling you to track and act on possible threats rather than individual alerts. You can then use the orchestration and automation capabilities in Azure Sentinel and through integration with other services, such as Azure Monitor Workbooks and Azure Logic Apps, to not only identify threats but also initiate actions when threats arise. Through Logic Apps, Azure Sentinel supports over 200 connectors to allow you to integrate with ticketing systems, messaging alerts, email alerts, and other systems and services to build automated response strategies for each threat.

To help you avoid threats altogether or mitigate them before they affect your environment, Azure Sentinel enables you to proactively hunt for threats across your entire environment and surface the results for follow-up and further investigation.

Finally, the Azure Sentinel community gives you access to workbooks, playbooks, hunting queries, and other resources that you can use in your own environment. You can also create custom resources to help you tune Azure Sentinel to your environment and specific needs.

Azure Dedicated Hosts

By default, even though your VM workloads are isolated from those deployed and used by other organizations, they are nevertheless potentially hosted on the same hardware. If you have regulatory or other compliance requirements that prevent you from deploying your VMs on shared hardware, or you simply want to add one more layer of isolation, you can deploy your VMs to dedicated hardware. To increase your security posture and reduce your threat profile, you can use Azure Dedicated Hosts for your virtual machines.

An Azure Dedicated Host is an Azure resource mapped to a physical server in Azure that you provision in an Azure region and optionally in an availability zone and fault domain. You create the dedicated host resource within a host group. Once the dedicated host is provisioned, you can deploy your VMs to it and, as indicated earlier, use availability zones and fault domains to provide high availability and fault tolerance. You can also use virtual machine scale sets for additional scalability and management. In the context of the AZ-900 exam, understand that Azure Dedicated Hosts provide the means for you to isolate your VM workloads on dedicated hardware, keeping them physically separate from VMs hosted by other organizations or from other VM resources that you host yourself.

Azure Governance Methodologies

The term *governance* encompasses a wide range of topics but generally describes policies and methods that control how a service is used, roles and responsibilities within the service, and how it should be secured. Azure offers several features to provide those capabilities within Azure, enabling you to build an Azure strategy that is secure, controlled, and manageable. The first of these governance features are *policies* and *initiatives*.

Azure Policies

Azure *policies* define business rules that you can use to assess and ensure compliance with organizational standards in Azure, controlling how Azure resources are deployed and used. The Azure Policy service provides the mechanism to create, manage, and apply those policies. You use functions, parameters, logical operators, conditions, and aliases when creating policies to define matching criteria. The policy service evaluates those criteria and determines what *effect* to apply to resources that match the policy criteria. Each policy applies a single effect, such as *deny*.

TIP

An Azure policy alias enables you to restrict the values and conditions permitted for a property of a given resource. Azure offers many predefined aliases.

TIP

Azure policies are created as JSON files.

Consider an example. Assume you want to ensure that only specific sizes of virtual machines are added to a resource group because you need to control costs. You want to make sure that instead of using a VM with lots of memory and other resources, you allow only VMs with limited resources to meet minimum service requirements. You can always scale as needed if demand increases. In this scenario, you create a policy for the resource group that restricts the types of VMs that can be added to the resource group. If someone attempts to add a VM that does not fit the accepted criteria, the action is denied (because you specify the *deny* effect in the policy).

TIP

Azure Policy includes many built-in policies that you can use across a wide range of categories, simplifying and speeding up policy implementation.

As discussed earlier, you specify the scope of a policy by assigning the policy to a specific scope object, such as a resource group or management group. The policy then applies to all child objects within that scope unless you exclude a specific subscope from the policy.

TIP

You do not apply permissions with Azure policies. Instead, you specify what actions people can take within a particular management scope using the permissions they already have. For example, a user might be granted permission to create resources in a resource group (using role-based access control, discussed later in this chapter). A policy applied to the resource group could then limit the types of VMs that the user could create in that group.

Azure Initiatives

An Azure *initiative* is a group (collection) of Azure policies. You use the initiative to achieve a collective set of governance goals. For example, perhaps you have an initiative to secure all SQL services in the organization. You would create an initiative for that goal, and then assign policies to that initiative. As with policies, you assign initiatives to specific scopes, so the policies in an initiative then apply to the resources that fall within the specified scope(s).

TIP

As with policies, Azure initiatives do not enable you to assign permissions. They simply serve as a container for policies. Since the policies do not apply permissions, neither do the initiatives that contain them.

When you apply an initiative to a scope, the policies contained in the initiative are evaluated and applied to all resources within that scope. You can also apply an initiative to multiple scopes, which means that all the resources in all the assigned scopes will have the policies evaluated and applied. If you need to have a policy evaluated by itself without other policies, either apply the policy outside of an initiative or create an initiative that contains only that policy.

TIP

Initiatives can contain only policies in a single subscription. To apply an initiative to resources in multiple subscriptions, create the same initiative within each subscription and apply each initiative as needed within each subscription.

Role-Based Access Control

Role-based access control (RBAC) is a primary authorization mechanism in Azure that enables you to define who has access to Azure resources and what they can do with those resources. For example, if yours is a large organization, you likely have a team responsible for networking, another team for managing VMs, another for databases and database servers, and so on. RBAC enables you to apply that role-based governance to your Azure resources. For example, you could use RBAC to enable the members of your SQL team to manage SQL Server VMs and Azure SQL Databases. Or, you might use RBAC to enable a Linux team to manage your Linux servers but not Windows servers, and vice versa.

You can use RBAC in many ways to control Azure management functions, including managing users, resources, VNets, and so on. Following is a list of some examples of how you might use RBAC:

- Allow your server team to manage VMs in a subscription and your network team to manage the virtual networks.
- Allow your DBA team to manage database VMs and databases in one or more resource groups.
- Allow a user to manage all resources in a particular resource group.
- Allow an application to access specific resources in a resource group.
- Allow a small group of users to manage users in Azure.

To apply RBAC, you first create a role assignment, which consists of three elements that effectively translate to who, what, and where:

- **Security principal:** Specifies the individual user, group, or managed identity to which the role assignment will apply.
- **Role definition:** A collection of permissions that specifies the operations that can be performed, such as read, write, and delete.
- **Scope:** Specifies the resources to which the role assignment applies.

Understanding Roles

Role definitions require some additional discussion to help you understand the actions that RBAC can govern. These roles are divided into three types: classic subscription administrator roles, Azure roles, and Azure AD roles. The classic subscription roles were the initial and only means of managing resources in Azure. Then, RBAC was introduced to provide much more granular control.

Classic subscription administrator roles include the following:

- **Account Administrator:** This is the billing owner. The Account Administrator can manage billing in the Azure portal, manage all subscriptions in an account (including creating new ones), change the billing for a subscription, and change the Service Administrator.
- **Service Administrator:** This role manages the services in the Azure subscription and can cancel the subscription and assign users to the Co-Administrator role.
- **Co-Administrator:** This role has the same privileges as the Service Administrator but cannot change the association of subscriptions to Azure directories. The role can also assign additional users to the Co-Administrator role, but cannot modify the Service Administrator.

Azure RBAC adds more granularity to permission assignment in Azure with over 70 built-in roles, many of which are specific to resource types. For example, the Virtual Machine Administrator Login role can view VMs in the Azure portal and log in as an administrator, but has no permissions to (for example) content delivery networks.

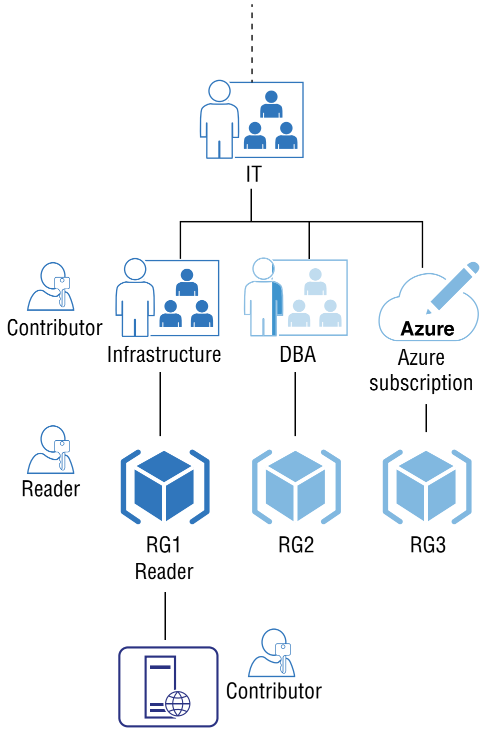
For the purposes of the AZ-900 exam, let's focus on the following four roles:

- **Owner:** This role has full access to all resources and can delegate access to others. The role applies to all resource types. Service Administrator and Co-Administrator roles have Owner permissions as the subscription scope.
- **Contributor:** This role can create and manage all types of Azure resources and create new tenants in Azure AD but cannot grant access to others.
- **Reader:** This role can view (consume) Azure resources. The role applies to all resource types.
- **User Access Administrator:** This role can manage access to Azure resources.

Using RBAC with Management Scopes

RBAC supports four levels of management scope: management group, subscription, resource group, and resource. In many cases, multiple role assignments will apply because a user or group will have overlapping role assignments. RBAC uses an additive model, which means your effective permissions are summed up across all assignments. For example, assume you have a role assignment that grants you Reader permission within a resource group. You also have a role assignment at the subscription level that gives you Contributor permission. Because the resource group is contained in the subscription and inherits permissions as a child, you effectively have Contributor permission on the resources in the resource group. Figure 4.6 illustrates this example.

FIGURE 4.6 RBAC uses an additive model to apply permissions.



Resource Locks

Creating and managing Azure resources can be a very complex task, particularly in large environments. Azure therefore gives you a means to lock down resources to prevent them from being modified or deleted. Resource locks are the Azure mechanism that enable you to apply that control.

You can apply a ReadOnly or a CanNotDelete lock. The ReadOnly lock enables authorized administrators to read a resource but not delete or update it. The CanNotDelete lock allows authorized administrators to read and modify a resource but not delete it.

Locking a resource does not lock it forever. If you need to delete a resource, you must first remove the lock. Then you can delete the resource. Resource locks are absolute in the sense that RBAC does not override a lock. Even if you own a resource and have full permissions to it, you cannot delete the resource if it is locked. Again, you must remove the lock first and then can delete it.

NOTE

You cannot apply locks in the context of specific users or roles. Applying a lock to a scope or resource applies the lock to all users, regardless of their RBAC roles and permissions.

Management scope also applies to resource locks, and when you apply a lock to a parent scope, all resources under that scope inherit the lock. For example, if you apply a ReadOnly lock on a resource group, all resources in that group inherit a ReadOnly lock.

If you apply locks for a resource at different scopes, the most restrictive lock applies. So, assume you apply a CanNotDelete lock on a resource group and then apply a ReadOnly lock for a resource in that group. Normally, the CanNotDelete lock would enable you to modify resources in the group but not delete them. Because the resource has a ReadOnly lock, however, you cannot modify the resource, even though the CanNotDelete lock would otherwise allow that.

TIP

Locks apply only at the resource management level, not at their functional levels. Assume that you apply a ReadOnly lock on a resource group containing Azure SQL Database instances, which then inherit that lock. You cannot modify or delete one of those database instances without removing the lock, but you can create new databases, as well as update and delete data within databases that exist in that resource group.

Azure Blueprints

Ensuring adherence to standards, patterns, and requirements is a key aspect of governance. For Azure, that means easily and effectively controlling deployment of resources based on resource groups, role assignments, policies, and Azure Resource Manager templates (which define the resources to deploy). Azure Blueprint is the Azure service that gives you this level of governance.

Azure Blueprint lets you define a repeatable group of Azure resources and associated role assignments and policies to meet your organization's standards and practices, and then quickly and easily deploy those resources where needed. Resource groups, role assignments, policies, and ARM templates are the *artifacts* within a blueprint that define its structure and enable a potentially large number of resources to be deployed collectively and in a controlled, standardized way.

Since Azure Resource Manager (ARM) templates also let you easily deploy resources, the capability to keep libraries of ARM templates would seem to offer the same capabilities as blueprints. However, ARM templates retain no connection to the resources they deploy. Blueprints do maintain that connection, so you can track and audit what *was* deployed against what the blueprint specified *should* be deployed. You can also implement changes to all resources and artifacts defined by a blueprint by updating, publishing, and applying a new version of a blueprint. Blueprints do not replace ARM templates. Instead, blueprints can make extensive use of ARM templates to deploy resources.

Blueprint Lifecycle

A blueprint is in draft mode until you publish it using a version designation that you define. Once published, a blueprint is available for assignment. Assigning a blueprint deploys the artifacts defined in the blueprint. So, simply updating and publishing a new version of a blueprint does not affect existing assignments; you must explicitly assign it after publishing it to apply changes.

A published version of a blueprint cannot be altered. If you need to modify the deployment, you create a new version of the blueprint with the appropriate changes, and then publish the new version and apply it. Applying the new version applies changes as defined in the new blueprint version.

You can delete a version of a blueprint only if it is not assigned. Deleting a blueprint version does not delete the other versions of the blueprint. You can also delete a core blueprint, but doing so deletes all versions of the blueprint. These cannot be deleted if they have active assignments, so you must remove assignments for each version of a blueprint before you can delete the core blueprint.

None of the resources defined in a blueprint are deleted when you unassign a blueprint version and delete that version, nor are they deleted when you delete a core blueprint. The resources are simply no longer managed or protected by the blueprint. However, some changes do occur:

- Blueprint resource locks are removed.
- Blueprint assignment object is deleted.
- The system-assigned management identity is deleted if one was used.

NOTE

When assigning a blueprint, you can choose to use a system-assigned managed identity, which then is granted an Owner role and is used to deploy resources defined by the blueprint.

Blueprint Roles

As you might expect, Azure provides role-based control over who can create, manage, and use blueprints. Azure includes the following built-in blueprint roles:

- **Owner:** Includes all Azure Blueprint permissions.
- **Contributor:** Can create and delete blueprint definitions but cannot assign blueprints.
- **Blueprint Contributor:** Can manage blueprint definitions but not assign them.
- **Blueprint Operator:** Can assign published blueprints but cannot create new blueprints.

TIP

You can create custom blueprint roles if you need permissions that are not provided by the built-in roles.

Microsoft Cloud Adoption Framework for Azure

As you have read through the preceding sections, you have probably realized that moving from an on-premises model to Microsoft Azure is not a trivial task, either in planning or in execution. The Microsoft Cloud Adoption Framework for Azure can help with both planning and execution.

The Cloud Adoption Framework for Azure is a large collection of resources, including documentation, deployment guidance, templates, best practice documentation, and various tools to help with planning, deploying, and assessing your Azure deployment.

The documentation included with the framework needs little explanation other than that it covers all aspects of planning and deploying Azure resources based on best practices. It includes guidance on strategies, governance, migration, innovation, and all other aspects of a successful Azure implementation. The framework documentation alone should be one of your first stops before moving to deploy Azure. But the documentation is just one aspect of the framework.

Of particular note as part of the Cloud Adoption Framework for Azure are the following:

- **Templates:** Within the framework you will find a wealth of templates to help you evaluate your business needs and build an Azure solution to meet them. Some of these templates are documents and others are live, interactive resources that you work through online to generate plans. Some templates work in conjunction with Azure Boards, a rich project workstream tool in Azure.
- **Assessments:** The Cloud Adoption Framework for Azure also provides multiple assessments to help you identify your cloud adoption plan based on business needs, remove blockers and improve processes, implement a sound governance framework, and ensure a well-architected Azure solution.

The framework site also provides information and links to additional resources to help you plan and deploy a sound Azure implementation. These include FastTrack for Azure, a Microsoft service that connects you with Microsoft engineers who help you work through planning and deployment considerations for Azure. The Azure Migration Program provides best practice and other guidance, access to training, Azure engineering support, migration tools, and access to migration partners to help you move your workloads to Azure.

TIP Visit `https://aka.ms/adopt` to learn more about the Microsoft Cloud Adoption Framework for Azure.

Azure Monitoring and Reporting Options

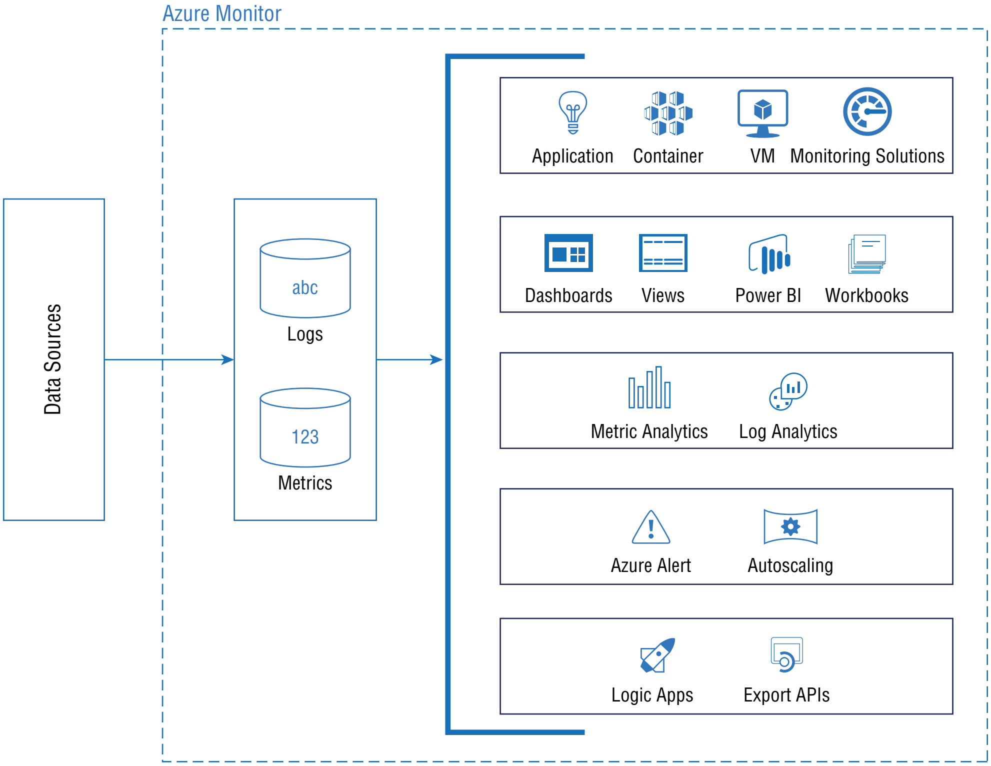
Monitoring and reporting are critical components of any IT environment, and Azure is no exception. This section of the chapter explores monitoring and reporting options in Azure.

Azure Monitor

Azure Monitor provides the capability to collect and analyze telemetry from your cloud and on-premises environments and to take appropriate actions based on that analysis. Azure Monitor encompasses several services (see Figure 4.7) that work together to provide a comprehensive monitoring and reporting solution:

- **Application Insights:** This feature enables developers to integrate monitoring for live applications by sending telemetry data to Azure. The data helps developers understand how an app is performing and how it is being used.
- **Azure Monitor for VMs:** This solution provides monitoring for Windows and Linux VMs in Azure, on-premises, and in other cloud environments.
- **Azure Monitor for Containers:** This solution provides monitoring for container workloads deployed to Azure Container Instances, Azure Kubernetes Services, and other container instances both in Azure and on-premises.
- **Log Analytics:** This tool provides the capability to write log queries and analyze query results.
- **Smart Alerts:** This solution automatically groups alerts using machine learning, combining alerts into a single issue to help minimize noise and enable management of related alerts.
- **Automated Actions:** Create actions that execute automatically in response to specific alerts, such as suppressing informational alerts during a planning maintenance window.
- **Dashboards:** Create and share dashboards to visualize the results of log queries.
- **Workbooks:** Create composite reports from multiple data sources to provide insights into performance, availability, resource usage, and more in an interactive report.

FIGURE 4.7 Azure Monitor encompasses multiple services and features to enable you to collect, analyze, and visualize events and metrics.



It is important to understand the types of data that Azure Monitor uses to learn how Azure Monitor functions and the roles it can play. These two data types are *metrics* and *logs*.

Metrics describe some aspect of a system at a given time using numerical values. As such, metrics are a snapshot in time of a specific characteristic of a resource. Two examples are the number of requests processed by Web Application Firewall and the amount of storage in bytes used by a storage account's file service.

Logs contain a record of events that happen within a system. Whereas metrics can only use numeric data to store information, logs can store a variety of data types in different structures, enabling logs to store more complex information. Logs are stored in tables within a Log Analytics workspace. You can build, edit, and run queries in Log Analytics to analyze log data.

TIP

Azure Monitor begins collecting data as soon as you add a resource to a subscription. You do not need to start the monitoring manually or configure any monitoring settings within the resource itself.

The key points to understand about monitoring and alerting in Azure, and about Azure Monitor in particular, in the context of the AZ-900 exam are as follows:

- Monitoring begins automatically as soon as you add a resource to a subscription.
- Metrics and logs are created for you automatically.
- Application Insights enables developers to send telemetry data about the applications they develop to Azure.
- Metrics are numeric values that describe how a resource is performing and/or what it is consuming.
- Logs contain detailed information about events that happen within your Azure environment.
- Log Analytics enables you to view data from multiple sources through queries that you create or that are created by services for you, such as On-Demand Assessments (available through Microsoft's Unified Support offering).

Azure Service Health

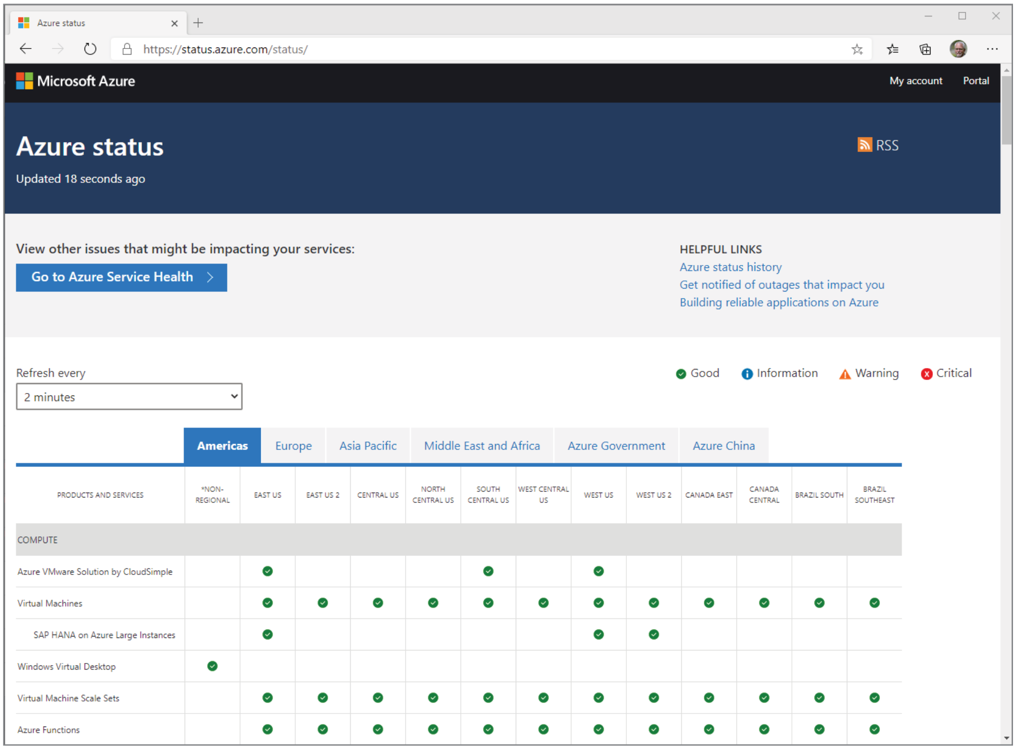
In a perfect world, nothing would ever go wrong. All your Azure resources and services would continue functioning optimally all the time and never overconsume their targets. But this is not a perfect world and things do go wrong on occasion. That is where Azure Service Health comes in.

Azure Service Health keeps you informed regarding planned maintenance and changes, Azure service issues that affect your environment, and issues within your own environment. Azure Service Health provides the following three features:

- **Azure Status:** This portal (see Figure 4.8) provides information on Azure services globally to help you see at a glance what services are affected and in what regions.
- **Service Health:** This service tracks the state of your Azure services by region and gives you access to information about service issues, planned maintenance, health advisories, and security advisories in a customizable dashboard (see Figure 4.9).
- **Resource Health:** This service, which is part of Service Health, tracks the state of the resources you have deployed to Azure to give you visibility to any ongoing or historical issues with those resources.

In addition to giving you a customizable dashboard to track the health of Azure services in the regions where your resources are located and get more information about issues, Service Health enables you to set up service health alerts. Service Health works with Azure Monitor to provide alerts through emails, text messages, and webhook notifications (to display alert information on your websites). You can use action groups, which are collections of notification preferences, to define actions and recipients who are notified when an alert is triggered. Action groups provide a means for building governance and consistency in how you deploy alerts in your organization and simplify creating your alerting process. You can create up to 2,000 action groups in a subscription.

FIGURE 4.8 Azure Status provides status information about Azure services worldwide.



Azure status

Updated 18 seconds ago

View other issues that might be impacting your services:

Go to Azure Service Health >

HELPFUL LINKS
Azure status history
Get notified of outages that impact you
Building reliable applications on Azure

Refresh every: 2 minutes

✓ Good ● Information ⚠ Warning ✕ Critical

Americas | Europe | Asia Pacific | Middle East and Africa | Azure Government | Azure China

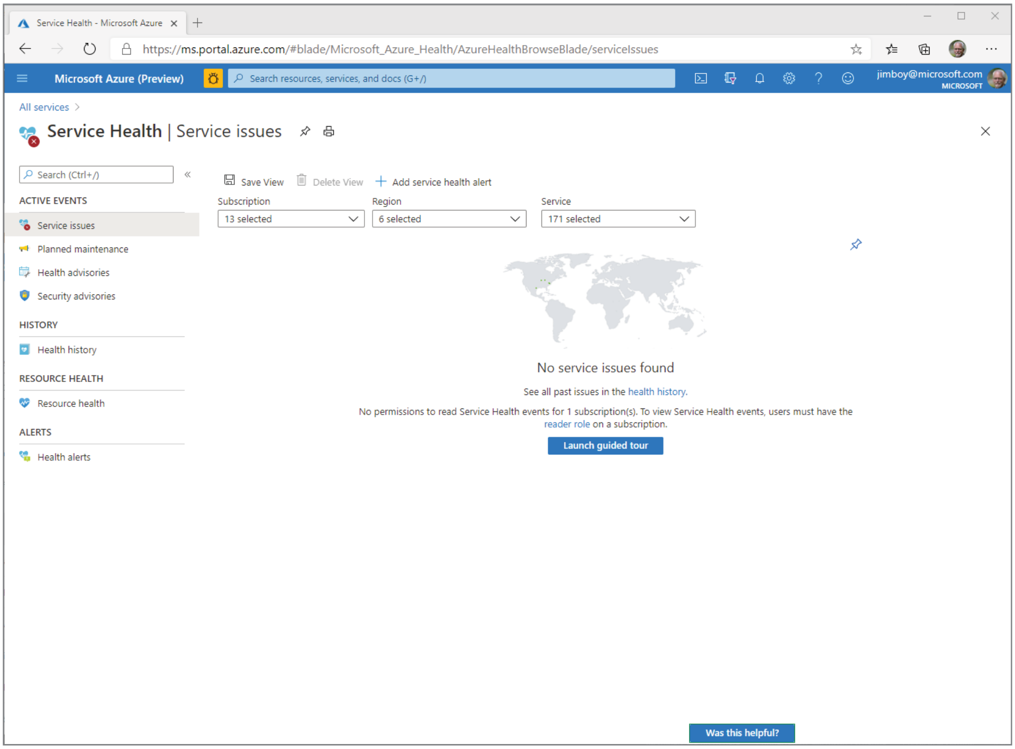
PRODUCTS AND SERVICES	*NON-REGIONAL	EAST US	EAST US 2	CENTRAL US	NORTH CENTRAL US	SOUTH CENTRAL US	WEST CENTRAL US	WEST US	WEST US 2	CANADA EAST	CANADA CENTRAL	BRAZIL SOUTH	BRAZIL SOUTHEAST
COMPUTE													
Azure VMware Solution by CloudSimple		✓				✓		✓					
Virtual Machines		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SAP HANA on Azure Large Instances		✓						✓	✓				
Windows Virtual Desktop	✓												
Virtual Machine Scale Sets		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Functions		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The last component of Azure Service Health to explore is Resource Health, which offers information about Azure issues that are affecting your resources or that have affected them in the past. You can use Resource Health to diagnose issues with your Azure resources to determine an appropriate course of action. For example, you can see if a resource is available or unavailable, view recent events such as an unplanned reboot of a system, or see whether a resource has experienced a degradation in performance. To view the Resource Health dashboard, open the Service Health portal and click Resource Health in the left navigation pane (Figure 4.10).

Azure Advisor

Azure Advisor is another resource you can use in Azure to improve the security posture of your environment. Azure Advisor, which you access through the Azure portal, provides a web-based report intended to help you optimize your Azure environment. The tool captures a wide range of data points across the environment, evaluating performance criteria, cost-effectiveness, reliability, security, and operational excellence. Azure Advisor offers guidance on ways to improve your deployments in those areas.

FIGURE 4.9 Service Health provides information on Azure service health, planned maintenance, and other information.



Subscription: 13 selected

Region: 6 selected

Service: 171 selected

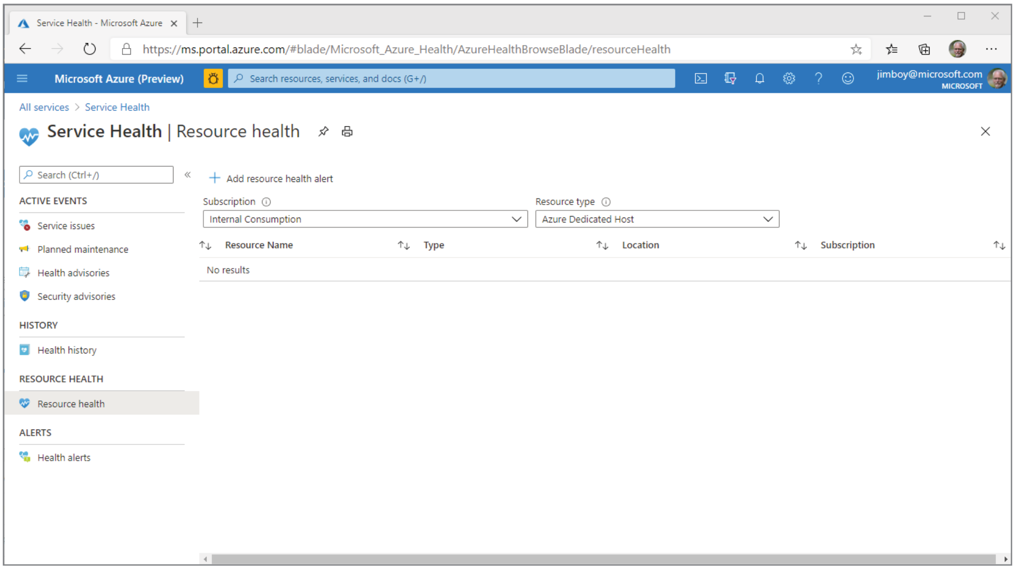
No service issues found

See all past issues in the health history.

No permissions to read Service Health events for 1 subscription(s). To view Service Health events, users must have the reader role on a subscription.

Azure Advisor Score is a feature in preview as of this writing that provides a score based on the analysis that Azure Advisor performs, similar to the secure score offered by Security Center. Addressing items identified by Azure Advisor in a positive way drives your score higher.

FIGURE 4.10 You can view health data for resources in your Azure environment in the Resource Health dashboard.


Service Health - Microsoft Azure
https://ms.portal.azure.com/#blade/Microsoft_Azure_Health/AzureHealthBrowseBlade/resourceHealth
Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
jimboy@microsoft.com
MICROSOFT
All services > Service Health
Service Health | Resource health
Search (Ctrl+/)
ACTIVE EVENTS
Service issues
Planned maintenance
Health advisories
Security advisories
HISTORY
Health history
RESOURCE HEALTH
Resource health
ALERTS
Health alerts
Add resource health alert

Subscription: Internal Consumption

Resource type: Azure Dedicated Host

Resource Name	Type	Location	Subscription
No results			

Compliance and Data Protection Standards

Key factors for many organizations when choosing a cloud solution are compliance, privacy, and adherence to data protection standards. This section explores these factors and the Azure services that support them. A good grasp of these topics begins with an understanding of common compliance standards and terms.

Industry Compliance Standards and Terms

Azure supports a broad range of compliance offerings. The following list describes the most common:

- **Health Insurance Portability and Accountability Act (HIPAA):** This is a US federal law that regulates protected health information (PHI) with a goal of protecting privacy surrounding individuals' health care.

- **International Organization for Standards (ISO):** ISO is a standards-based, nonregulatory organization located in the United States.
- **International Electrotechnical Commission (IEC):** IEC is a nonprofit, nonregulatory standards organization based in Geneva, Switzerland.
- **National Institute of Standards and Technology (NIST):** NIST is a nonregulatory agency of the US Department of Commerce. Until 1998, NIST was known as the National Bureau of Standards.
- **General Data Protection Regulation (GDPR):** The General Data Protection Regulation defines data protection and privacy requirements as a regulation in European Union (EU) law. It applies to personal data of individuals who are in the European Economic Area (EAA) and to any enterprise that processes data of individuals in the EAA.

Some of these standards are discussed in more detail in the context of Azure in following sections of this chapter. For now, understand that these compliance offerings fall into two categories: regulatory and nonregulatory. GDPR is an example of a regulatory requirement that is enforced by a governmental body (in this case, the EU). ISO, IEC, and NIST are nonregulatory organizations that define standards but do not regulate or enforce them.

Microsoft Privacy Statement

The Microsoft Privacy Statement located at `https://privacy.microsoft.com/privacystatement` describes not only what personal data processes, but also how and why.

Anything other than anonymous access requires a login account, and this includes Microsoft 365, Azure, and other resources like the Windows Store, Volume Licensing Service Center, support portals, and other resources provided by Microsoft. With Azure, your user login will reside in Azure AD. The same is true with Microsoft 365. Whether you use a personal email or work email to establish that user account is situation specific. In an enterprise, your account will be tied to your work email address. You might also be using a Microsoft account to access some services, such as the Windows Store or Xbox Live. Microsoft accounts can be tied to a personal email account, a work or school account, or an account set up for you by a third party, such as your Internet provider.

Regardless of the account type, some Microsoft products and services require that you provide a user account. In that sense, those products and services require you to provide your personal information, and without that, you are unable to use the product or service. This is required in some cases by law and in others is required to establish a contract between you and Microsoft. Using a service such as Xbox Live is an example of the latter.

There are multiple levels of privacy protection for you defined within the Microsoft Privacy Statement, but privacy is not absolute. Microsoft can share your personal information with vendors working on Microsoft's behalf, Microsoft-controlled subsidiaries and affiliates, and others when required by law or in response to a legal process. Obtaining support for a product is an example. Microsoft might contract with a vendor to provide support for a product to supplement its own support resources. Without some personal information, the vendor would be unable to provide support.

Online Service Terms

The Azure Online Service Terms (OST), which is a legal agreement between an Azure customer and Microsoft, details the obligations for the organization and Microsoft in the processing and security of personal and customer data. The OST covers not only Azure, but also Office 365, Dynamics 365, and Bing Maps. You will find the OST at `www.microsoft.com/licensing/terms/product/ForallOnlineServices`.

Data Protection Addendum

The Data Protection Addendum (DPA) adds to the definition of obligations detailed in the OST. It defines the terms for legal compliance, disclosure of processed data, data security practices and policies, data encryption, data access, and audit compliance. The DPA also defines terms for data transfer, retention, and deletion. You can find the DTA by navigating to `www.microsoftvolumelicensing.com/DocumentSearch.aspx` and searching for DPA.

NOTE The Microsoft Privacy Statement, the Online Service Terms, and the Data Protection Addendum encompass Microsoft's terms for protecting customer data and privacy across its cloud offerings.

Trust Center

Microsoft Trust Center is a website that provides information about how Microsoft implements and supports compliance, security, privacy, and transparency across its cloud products and services. The site is located at `www.microsoft.com/trustcenter`. Trust Center is intended to help you design and implement a secure Azure solution.

Understanding that Trust Center contains a wide range of security information is a key certification topic, but understanding what Trust Center is *not* is also important. Trust Center does not provide any type of risk assessment for your Azure resources and services—Compliance Manager fulfills that function. Nor does Trust Center offer best practice recommendations for hybrid Azure implementations—Azure Security Center provides those recommendations. Last, Trust Center does not enable you to configure or enforce compliance settings or define policies—that is a function of Azure Policies.

In summary, Trust Center is a website containing information about security, privacy, compliance, transparency, and related products and services.

Service Trust Portal

Service Trust Portal is a public site through which Microsoft publishes audit reports and other compliance-related information for its cloud services, including Azure. You can use Service Trust Portal to download audit reports required by your organization or by third-party auditors and access reports that describe how Microsoft builds and manages Azure, Microsoft 365, and Dynamics 365. Service Trust Portal also offers information to help you understand how Azure can help you meet standards and regulations defined by ISO, NIST, GDPR, and others.

TIP

The Service Trust Portal is located at `https://servicetrust.microsoft.com`.

Service Trust Portal also hosts the Compliance Manager, which is described in the following section.

Compliance Manager

Compliance Manager is a dashboard published through the Service Trust Portal that enables you to view compliance information and track compliance-related activities, including the following:

- View information provided by Microsoft to third-party auditors and regulators detailing compliance for various standards.
- View information compiled by Microsoft to demonstrate Microsoft's compliance with various regulations.
- View your organization's compliance self-assessment and score.
- Assign and track compliance-related activities within your organization.
- Maintain a secure repository for your compliance audits and related evidence for compliance activities and outcomes.
- Access detailed compliance report documents to provide to internal stakeholders and third-party auditors and regulators.

Compliance Manager uses a workflow-based risk assessment to develop your organization's assessment score. As described briefly in the previous list, Compliance Manager enables you to build a compliance framework where you can create and assign compliance-related tasks to individuals in your organization and track progress toward completion of those activities.

NOTE

Compliance Manager can offer recommendations for helping you achieve compliance goals and requirements, but it cannot guarantee compliance. Responsibility for compliance ultimately falls to your organization.

Azure Government

The US government has strict requirements for data privacy, isolation, compliance, and security. Microsoft created Azure Government to meet those requirements. Azure Government is a separate instance of Azure with data centers only in the United States to support US federal agencies, state and local governments, and solution providers that support these governmental entities. Azure Government is physically isolated from commercial Azure and is supported and managed by screened US personnel. Deployments to Azure Government are subject to validation of eligibility.

NOTE

Azure Government and Azure China are referred to as Azure Sovereign Regions because they are specific to the United States and China, respectively.

Services in Azure Government and in commercial Azure are mostly the same, and the user experience is also generally the same. For example, the Azure portal offers the same user experience in both environments, but they are accessed through different URLs.

Hosting resources in Azure Government does not in itself meet specific governmental compliance requirements. Although Azure Government does meet broad compliance requirements and Level 5 Department of Defense (DoD) approval, you must ensure that your organization's implementation of Azure meets all compliance requirements.

TIP

As with commercial Azure, Microsoft deploys Azure Government in regions. A region can be a commercial region or a government region, but not both. Data centers located in a government region host only government resources.

Azure China

Chapter 1, "Cloud Concepts," briefly described Azure China, a physically isolated instance of Azure located in China and designed to meet strict Chinese regulations. Azure China is independently operated by Shanghai Blue Cloud Technology Co., Ltd. (commonly known as 21Vianet). Azure China must be hosted and managed by 21Vianet due to a Chinese requirement that providers of cloud services must have a value-added telecom permit. To qualify for a permit, a company must have less than 50 percent foreign investment. 21Vianet therefore licenses Azure technologies from Microsoft.

Azure China is available to any organization that needs to host resources and services in China. Azure China is not restricted to Chinese government agencies or companies. Instead, it is intended for any organization doing business in China that needs to meet Chinese regulations.

Connectivity is another consideration. Assume that your organization needs to establish a presence in Azure China but also needs interconnectivity with your on-premises network in China or with Azure. The following list summarizes the two possible scenarios:

- **Within China:** You can use ExpressRoute to establish a secure connection between Azure China and your on-premises data center or private cloud located within China. ExpressRoute is not supported for direct network connectivity to sites outside of China or to Azure outside of China.
- **Outside of China:** Establish a site-to-site VPN between Azure China to a location outside of China.

Regardless of which scenario applies, you must acquire the VPN or ExpressRoute service from telecom providers licensed by the Chinese Ministry of Industry and Information Technology (MIIT).

Portability is a final consideration for Azure China. Because of differences in services, pricing, and regulations, you cannot move Azure accounts from Azure to Azure China. You must create a separate Azure China account. Cross-border data transfer is also subject to security assessment and government approval.

Summary

This chapter explored several topics related to network security, authentication and authorization, governance methodologies, and data protection and compliance standards in Azure. All of these resources and services help ensure your Azure environment is not only secure from threats, but also designed with an appropriate governance model to protect resources from modification, whether intended or unintended, and ensure that resources are deployed and managed using the standards and requirements established by your organization. Governance is an extremely important aspect of planning and deploying an Azure solution and should be considered early and often.

Azure offers many tools and features to help you both implement and assess security. These include Security Center, Key Vault, Azure Information Protection (AIP), and Advanced Threat Protection (ATP). Azure also offers tools for ensuring adherence to compliance and data protection standards through Trust Center, Service Trust Portal, and Compliance Manager.

You also learned a bit more about Azure Government and Azure China, both of which are designed to meet stringent government regulations and requirements in the United States and China, respectively.

Exam Essentials

Describe securing network connectivity in Azure. Azure Firewall provides broad-based firewall coverage for networks and resources in Azure and are often deployed in concert with other network security services. Use Azure Firewall when you need to filter traffic based on IP address, port, and/or protocol.

Web Application Firewall (WAF) works in concert with Application Gateway, Front Door, and CDN and is specific to web application scenarios. For services other than web applications, turn to Azure Firewall and network security groups.

Network security groups (NSGs) are deployed at the subnet or VM level to provide traffic filtering at those levels. NSGs filter traffic based on protocol, source address, source port, destination address, and destination port. You will often use NSGs in concert with application security groups.

Application security groups (ASGs) enable you to group servers based on the applications running on them and manage security for them as a group. An ASG is an object reference within an NSG, making it easy to apply rules to the VMs contained within an ASG.

User-defined routes (UDRs) enable you to create custom routes to direct traffic through non-default routes.

Azure DDoS Protection provides a means of protecting against distributed denial-of-service attacks. DDoS Basic offers active traffic monitoring and automatic attack mitigation. DDoS Standard adds an SLA, mitigation policies, metrics and alerts, and reporting.

Describe core Azure identify services. Azure AD provides identify management for Azure, enabling users to log into cloud services such as Office 365 and access resources in Azure. Azure AD Free provides management of users and groups, synchronization with on-premises AD, basic reporting, and self-service password change for Azure AD accounts, along with single sign-on (SSO) for Azure, Microsoft 365, and Dynamics 365. Azure AD Premium includes additional features such as the ability to authenticate to on-premises resources, self-serve password reset for on-premises users, dynamic groups, and more.

Authorization goes hand in hand with authentication. Whereas authentication identifies the user, authorization determines whether an identified user is authorized to use a resource.

Describe security tools and features of Azure. Azure offers many tools and resources for ensuring security. Azure Security Center provides monitoring, alerts, and recommendations for security risks for both Windows and Linux systems. Security Center integrates with Microsoft Defender to provide risk detection and assessment. Security Center automatically discovers and assesses resources when you deploy them.

Azure Key Vault provides a secure repository for certificates, keys, and other secrets, along with the capability for applications to call Key Vault to access stored secrets when needed. You can also create and manage secrets with Key Vault.

Azure Information Protection (AIP) uses rights management and labels to classify and optionally protect documents and emails with encryption, identity, and authorization.

Advanced Threat Protection (ATP) leverages on-premises Active Directory to detect and identify threats directed at your organization. ATP protects against reconnaissance attacks, compromised credentials, lateral account movement, and domain dominance attacks.

Describe Azure governance methodologies. Azure offers several features to help you design and enforce a governance model. Azure policies define business rules that you use to control how Azure resources are deployed and used, providing a mechanism to create, manage, and apply policies. An Azure initiative is a group of policies that you create and deploy to meet a collective governance goal.

Role-based access control (RBAC) is a primary authorization mechanism in Azure that enables you to define who has access to Azure resources and what they can do with those resources. You apply RBAC by creating a security principal if one does not already exist, assigning a role definition, and defining the scope to which the role assignment applies. Azure includes many predefined roles, with the most common being Owner, Contributor, Reader, and User Access Administrator. Permissions granted through RBAC are additive.

Resource locks enable you to control what actions can be performed on resources. You can apply a ReadOnly lock that enables authorized administrators to read a resource but not delete or update it. CanNotDelete enables authorized administrators to read and modify a resource but not delete it. The most restrictive lock applies when locks are applied at different scopes.

Azure Blueprints enables you to define a repeatable group of Azure resources and associated role assignments and policies, and then quickly and easily deploy those resources where needed. A blueprint is in draft until published and must then be assigned to a resource group to apply it to those resources. Although removing an assigned blueprint does not delete resources, doing so does impose some changes, including removing resources locks, deleting the blueprint assignment object, and deleting the system-assigned management identify if one was used.

Describe monitoring and reporting options in Azure. Azure Monitor is a group of services and features that work in concert to provide a robust reporting, analysis, and alerting capability in Azure. Azure Monitor uses logs and metrics to capture data. Metrics are numeric values that describe how a resource is performing or what it is consuming. Logs capture data about events that happen in Azure. Monitoring begins automatically when you add a resource to a subscription; you do not need to configure logs or metrics manually. You can view reports with Azure Log Analytics. You can create custom queries and use dashboards to visualize the results of your queries.

Application Insights enables developers to send telemetry data from your custom applications to Azure, where that data can be consumed for monitoring and reporting.

The Azure Status portal provides a view of the global health state for Azure services by geography and region. Azure Service Health provides information on the health of Azure globally and of your resources deployed in Azure. Resource Health is a component of Service Health and shows information about resources you host in Azure.

Describe privacy, compliance, and data protection standards in Azure. Azure provides many features to enable organizations to meet standards, both regulatory and nonregulatory, in their Azure environments. Nonregulatory organizations such as ISO, IEC, and NIST produce and publish standards but do not enforce them through regulations. HIPAA and GDPR are examples of regulations that are enforced by government agencies or governmental bodies.

The Microsoft Privacy Statement describes the personal data that Microsoft processes, as well as how and why they process it. Using some Microsoft services requires providing personal data. Microsoft can and does share some personal data with its vendors, subsidiaries, and affiliates, and with others when required by law or in response to a legal process.

Trust Center is a Microsoft website containing information about security, privacy, compliance, transparency, and related products and services. Trust Center does not provide any type of risk assessment for your Azure resources and services, nor does it offer risk assessments or enable you to configure or apply compliance settings or policies.

Service Trust Portal is a public site that you use to access audit and compliance reports for Azure. You can also access information to help you understand how to meet standards and regulations. Service Trust Portal also hosts Compliance Manager.

Compliance Manager enables you to view information that Microsoft provides to third-party auditors to demonstrate compliance. You can also use Compliance Manager to build a compliance framework and assign and track compliance tasks for your organization. Compliance Manager also uses a workflow-based risk assessment to develop your organization’s compliance score.

Azure Government is an isolated instance of Azure supporting US federal agencies, state and local governments, and solution providers that serve these governmental entities. Azure Government is supported and managed by screened US personnel.

Azure China is an isolated instance of Azure supporting organizations that need to host Azure resources within China. Azure China is hosted and supported by 21Vianet under license from Microsoft. Azure China is not restricted to Chinese government entities or Chinese companies. Data connections between Azure China and other sites inside China require ExpressRoute. Connections between Azure China and sites outside of China require a site-to-site VPN. In both cases, the connection must be made by a telecom provider licensed by the Chinese Ministry of Industry and Information Technology.

Review Questions

1. You are setting up resources in Azure and need to filter traffic based on source IP address and port, destination IP address and port, and protocol between your on-premises network and Azure. Which of the following meets these minimum requirements?

   A. ExpressRoute

   B. Azure Firewall

   C. Application security groups

   D. User-defined routes

2. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

   You are evaluating moving a web application that you host on-premises to Azure. The solution comprises three VMs—a web front end, an application server, and a database server. You need to ensure that your administrators can access all of the VMs for remote management on port 3389, but only the web front end should be accessible over port 80. You decide to deploy an application security group to protect the web server and enable access to the other servers.

   A. deploy Web Application Firewall to filter and route traffic to the web server and deploy network security groups to enable RDP to all three VMs.

   B. deploy Web Application Firewall to filter the traffic and meet both requirements.

   C. deploy a network security group to filter traffic and meet both requirements.

   D. No change is needed.

3. You have deployed a VM to a subnet in Azure and need to ensure that only your and one other individual can connect to the VM using RDP on port 3389 to manage it. No other access from outside the subnet should be allowed at this time on any other ports. Which of the following should you use? (Choose all that apply.)

   A. Use a network security group to filter traffic and only allow port 3389 to the VM.

   B. Apply an Azure policy to the subnet to limit access on port 3389 to only your and your peer's accounts.

   C. Create a policy initiative that restricts access to the server based on your and your peer's roles, and to port 3389 for the IP address of the VM.

   D. Use role-based access control (RBAC) to ensure that only you and your peer can access the server.

4. You are considering deploying a key web application to Azure. You decide to deploy Web Application Firewall with Application Gateway as part of the project. Which of the following correctly describes the function of Web Application Firewall in this scenario?

   A. When properly configured, it ensures that traffic reaches the application only on port 80 for HTTP traffic.

   B. It protects the web application from common web-based attacks.

C. It ensures that users can reach the web service on port 80 and administrators can RDP to the VMs on port 3389.

D. None of the above.

5. Your organization hosts a VM that performs a security-related function. For both security and auditing purposes, you need to ensure that all traffic reaches the VM from a single IP address in another subnet, regardless of source. Which of the following solutions meets this requirement?

A. Create a network security group (NSG) that directs all traffic for the VM to the designated IP address and then apply the NSG to all subnets as required.

B. Create an application security group (ASG) that directs all traffic for the VM to the designated IP address and apply the ASG to all subnets in the virtual network.

C. Create a user-defined route as a custom routing table and apply the table to all subnets in the virtual network.

D. Use rules in Azure Firewall to route traffic to the target VM based on source and target IP addresses.

6. Which of the following describes Azure DDoS Protection Standard? Choose all that apply.

A. It protects against volumetric, protocol, and resource layer attacks.

B. It alerts you when an attack is happening.

C. DDoS Standard protects all resources on a virtual network as soon as the service is enabled.

D. It provides mitigation reports.

7. Your organization has made the decision to move workloads into Azure. As the Directory Services administrator, you need to explain authentication and authorization in Azure to the program managers leading the project. Which of the following are correct statements?

A. Identifying a user by a username and password is a form of authorization.

B. Validating that a user account has the necessary permissions to access a resource is an example of authorization.

C. Authentication identifies a user but does not provide access to resources.

D. Providing a password to access a shared resource is a form of authorization.

8. Which of the following is the least expensive option that enables Azure AD users to change their passwords online?

A. Azure Active Directory Base

B. Azure Active Directory Free

C. Azure Active Directory Premium P1

D. Azure Active Directory Premium P3

9. Which of the following correctly describe Azure Active Directory? (Choose all that apply.)

A. Azure AD is a key component of role-based access control (RBAC) in Azure.

B. You must register an Azure web application with Azure AD to enable that application to authenticate and authorize users.

C. All editions of Azure AD enable management of users and groups.

D. You must use on-premises Active Directory along with Azure AD to enable on-premises users to authenticate in Azure.

10. Which of the following capabilities require an Azure AD Premium edition? (Choose all that apply.)

A. Self-service password management for on-premises users, enabling them to change their own passwords

B. Enabling users to access on-premises resources such as an on-premises website using an Azure AD account

C. Managing Azure AD groups

D. Using RBAC to control access to resources with policies and initiatives

11. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

Entering your PIN after you insert a debit card into an ATM is an example of multifactor authentication (MFA).

A. Providing a username and password to log into Windows.

B. Entering a PIN code on a keypad to enter a building.

C. Providing an email address and password to log into a website.

D. No change is needed.

12. Which of the following are correct statements regarding Azure Security Center? (Choose all that apply.)

A. Security Center integrates natively with Microsoft Defender to provide risk detection and assessment.

B. Security Center supports Linux operating systems.

C. You must add resources to Security Center to begin monitoring those resources.

D. Security Center provides monitoring and threat protection for VMs in Azure as well as on-premises.

13. You are tasked with explaining some of the security options in Azure to your CIO, who has asked about how Azure will improve security over your on-premises environment. Which Azure service provides security recommendations for securing your Azure resources?

A. Advanced Threat Protection (ATP)

B. Azure DDoS Protection

C. Security Center

D. Azure Service Health

14. You are moving a SQL Server Analysis Services (SSAS) solution from on-premises to Azure to support custom reporting through Power BI. You want to enable access only when a report creator needs to query for data. Which Azure service supports just-in-time (JIT) access control, enabling users to gain access to the server for only a specified period of time?

A. Advanced Threat Protection

B. Security Center

C. Azure Key Vault

D. Azure Service Health

15. Which of the following accurately describe Azure Key Vault? (Choose all that apply.)

A. Provides the capability to create, manage, and store certificates and other secrets.

B. Provides highly secure storage for certificates and other keys but not the capability to create them.

C. Works in conjunction with Azure Threat Protection (ATP) to secure and contain certificate-based threats.

D. Enables application developers to avoid storing credentials in an application.

16. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

Azure Information Protection (AIP) enables organizations to protect emails and documents using encryption, identity, and authorization policies.

A. encrypts data stored in Azure Premium storage.

B. provides secure storage for certificates, cryptographic keys, and other secrets.

C. is a mechanism in Azure Active Directory for encrypting and securing administrator credentials.

D. No change is needed.

17. Which of the following Azure services can identify suspicious activities such as pass-the-hash attacks?

A. Security Center

B. Azure Information Protection (AIP)

C. Azure Advanced Threat Protection (ATP)

D. Microsoft Defender

18. Which of the following threats can ATP help you detect?

A. Reconnaissance attacks

B. Pass-the-hash

C. Pass-the-token

D. All of the above

19. Which of the following is an example of a honeytoken attack?

A. Testing multiple passwords against a username

B. Authentication attempts against an alphabetical list of usernames

C. Login to a fake account that you created

D. None of the above

20. You want to ensure that the VMs created in a resource group do not exceed certain limits for cores and other resources to reduce costs. Which of the following Azure features enables you to control this?

A. Resource locks

B. Azure policies

C. Azure Resource Manager

D. Azure initiatives

21. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

Azure initiatives <u>enable you to build blueprints to define how resources should be created and deployed in your Azure environment.</u>

A. control how blueprints are published and assigned to resources.

B. enable you to manage and implement policies as a group to achieve governance goals.

C. define security policies that you apply using Azure Security Center.

D. No change is needed.

22. Which of the following are correct statements describing Azure policies? (Choose all that apply.)

A. You can apply policies individually to a resource or within an Azure initiative.

B. You can apply permissions using policies to determine what actions a user can take against a resource.

C. Applying a policy to resource group causes the policy to apply to all resources within that resource group.

D. Azure policies are a component of Security Center that enables you to define security-related policies to protect resources.

23. Which of the following enable you to assign permissions to enable users to create and/or use resources in Azure?

A. Azure policies

B. Resource groups

C. Role-based access control (RBAC)

D. Security Center

24. You need to delegate the capability to add users in Azure to another individual at your organization. Which of the following RBAC roles should you apply to the user to provide this capability to manage management groups with the least privilege?

A. Owner

B. User Access Administrator

C. Contributor

D. Account Administrator

25. What is the role you should use to grant users the capability to create and manage resources in Azure while ensuring they have the fewest permissions needed?

A. Creator

B. Reader

C. Owner

D. Contributor

26. Which of the following statements accurately describe Azure locks? (Choose all that apply.)

A. An administrator with sufficient permissions in an RBAC role can override locks.

B. If you apply a lock to a resource group, the lock applies to all resources in the group, including any new resources that you create in the resource group.

C. The most restrictive lock applies in a situation where multiple locks are applied at different scopes.

D. You can delete a locked resource only after removing the lock, unless you have been assigned the Owner role.

27. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

The CanNotDelete lock is more restrictive than the ReadOnly lock.

A. prevents administrators from modifying a resource.

B. enables administrators to read but not modify a resource.

C. is less restrictive than the ReadOnly lock.

D. No change is needed.

28. Which of the following statements are correct regarding Azure Blueprints? (Choose all that apply.)

A. Azure Blueprints use Azure Resource Manager (ARM) templates to deploy resources.

B. Azure Blueprints let you define a repeatable group of Azure resources and associated role assignments and policies.

C. A blueprint does not take effect until you publish the blueprint.

D. Azure provides multiple roles for creating and managing blueprints.

29. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

When you delete a blueprint, all of the resources defined in the blueprint are deleted.

A. all versions of the blueprint are deleted.

B. none of the resources defined in the blueprint are deleted.

C. you must publish the change for it to take effect.

D. No change is needed.

30. Which of the following statements regarding blueprints are accurate? (Choose all that apply.)

A. All assignments of a blueprint are updated when you publish a new version of the blueprint.

B. When you unassign a blueprint, no resources defined in the blueprint are deleted but resource locking is removed.

C. A user with the Blueprint Contributor role can manage and publish blueprints.

D. You can delete a blueprint only if you unassign it first.

31. Which of the following statements about Azure Monitor is not correct?

A. Azure Monitor begins monitoring resources as soon as you create a resource.

B. Azure Monitor begins monitoring resources as soon as you create metrics and logs for them.

C. Application Insights enables developers to send telemetry data about the applications they develop in Azure.

D. Azure Monitor supports Windows and Linux operating systems.

32. You are an Azure administrator and want to view status information for the resources that you host in Azure, by region. Which of the following resources should you use for that purpose?

A. Azure Status

B. Azure Service Health

C. Resource Health

D. Azure Portal

33. Which of the following would you use to view information about planned maintenance in Azure?

A. Azure Monitor

B. Azure Security Center

C. Azure Advisor

D. Azure Service Health

34. Which of the following statements are correct about Azure Service Health? (Choose all that apply.)

A. Azure Service Health includes Azure Status, Service Health, and Resource Health.

B. You can set up service health alerts to send email and text notifications regarding items collected by Azure Monitoring.

C. You can use Service Health to publish Azure alerts to a website using webhooks.

D. You can create customizable dashboards in Azure Service Health to track the health of your resources.

35. Which of the following are standards-based, nonregulatory organizations or agencies? (Choose all that apply.)

A. NIST

B. ISO

C. GDPR

D. HIPAA

36. Which of the following statements is true? (Choose all that apply.)

A. You must provide personal information to use some Microsoft products.

B. Microsoft cannot share your personal information with any third party.

C. You cannot use a work email when setting up a Microsoft account that you will use to access Microsoft services.

D. You must use a personal email account when setting up a Microsoft account.

37. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

The Microsoft Trust Center enables you to view a broad range of security information about Azure and access risk assessments for your Azure resources.

A. enables you to establish high-level initiatives and policies to drive security and compliance.

B. enables you to view audit and compliance reports published by Microsoft.

C. is a website that provides information about how Microsoft implements and supports compliance, security, privacy, and transparency across its cloud offerings.

D. No change is needed.

38. You are a compliance manager for your organization, which has decided to move several services from your on-premises data center into Azure. Which of the following should you use to view audit reports published by Microsoft to assure your CIO that Azure offers a secure and compliant platform?

A. Trust Center

B. Compliance Manager

- **C.** Service Trust Portal
- **D.** Azure Compliance Portal

39. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

Compliance is the sole responsibility of Microsoft.

- **A.** is the sole responsibility of organizations that host their services in Azure.
- **B.** is a shared responsibility between your organization and Microsoft.
- **C.** is guaranteed by SLAs in Azure.
- **D.** No change is needed.

40. Which of the following statements are correct regarding Azure Government? (Choose all that apply.)

- **A.** Azure Government is an isolated instance of Azure in the United States.
- **B.** Azure Government is only available to governmental entities in the United States.
- **C.** Hosting in Azure Government meets all governmental compliance requirements.
- **D.** Resources deployed to Azure Government are hosted in data centers that are separate from nongovernment resources.

41. Which of the following statements are correct regarding Azure China?

- **A.** Azure China is available only to Chinese governmental agencies and solution providers that support them.
- **B.** Azure China is an isolated instance of Azure managed by Microsoft.
- **C.** You can easily move resources and Azure accounts from Azure to Azure China, and vice versa.
- **D.** A Chinese company, 21Vianet, manages Azure China.

42. Which of the following provides broad guidance, tools, and assessments to help with a migration of workloads to Azure?

- **A.** FastTrack for Azure
- **B.** Azure Advisor
- **C.** Cloud Adoption Framework for Azure
- **D.** Azure Migration Planning Service

Chapter

5

Azure Solutions

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

DESCRIBE CORE SOLUTIONS AND MANAGEMENT TOOLS ON AZURE

✓ **Describe core solutions available in Azure**

- Describe the benefits and usage of Internet of Things (IoT) Hub, IoT Central, and Azure Sphere
- Describe the benefits and usage of Azure Synapse Analytics, HDInsight, and Azure Databricks
- Describe the benefits and usage of Azure Machine Learning, Cognitive Services, and Azure Bot Service
- Describe the benefits and usage of serverless computing solutions that include Azure Functions and Logic Apps
- Describe the benefits and usage of Azure DevOps, GitHub, GitHub Actions, and Azure DevTest Labs